

LAW OFFICE OF MICHAEL L. FRADIN  
Michael L. Fradin, Esq.  
8401 Crawford Ave. Ste. 104  
Skokie, IL 60076  
Telephone: 847-986-5889  
Facsimile: 847-673-1228  
Email: mike@fradinlaw.com

Attorney for Plaintiff Foster

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO  
EASTERN DIVISION

TROY FOSTER; individually, and on  
behalf of all others similarly situated,

Plaintiff Foster,

v.

HEALTH RECOVERY SERVICES,  
INC.,

Defendant.

Case No. 2:19-cv-04453

**FIRST AMENDED COMPLAINT**  
**DEMAND FOR JURY TRIAL**

RULE 23 CLASS ACTION

Judge Algenon L. Marbley  
Magistrate Judge Jolson

**FIRST AMENDED COMPLAINT**

**INTRODUCTION**

Plaintiff Troy Foster (referred to herein as “Plaintiff”), individually and on behalf of himself and all others similarly situated, brings this Class Action Complaint against Defendant Health Recovery Services, Inc. (referred to herein as “HRS”) based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents, as to all other matters:

## **PARTIES**

1. Plaintiff Troy Foster is a resident of Athens, Ohio. He is, and was during the period of the Defendant HRS' data breach, a citizen of the State of Ohio. Plaintiff Foster was a recipient of services from Health Recovery Services, Inc., and thus had his Personal Information compromised as a result of Defendant HRS' data breach.

2. Defendant Health Recovery Services, Inc. is an Ohio private non-profit 501(c)3 corporation with its principle place of business in Athens, Ohio. Defendant HRS' website states that its mission involves "serving those affected with mental illness and alcohol, tobacco, and drug addiction." Defendant HRS states that they offer "both outpatient and residential treatment options for consumers."

## **JURISDICTION AND VENUE**

3. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million exclusive of interest and costs. At least one Plaintiff and one Defendant are citizens of different states. There are more than 100 putative class members.

4. This Court has personal jurisdiction over Defendant Health Recovery Services, Inc. because they regularly conduct business in Ohio and have sufficient minimum contacts in Ohio.

## **GENERAL ALLEGATIONS**

5. Defendant Health Recovery Services, Inc. is an Athens, Ohio based provider of alcohol and drug addiction services. In providing these services, Defendant HRS collects and stores the Personal Information of recipients of these services. This Personal Information includes, but is not limited to, names, addresses, telephone numbers, dates of birth, medical information, health insurance information, diagnoses, treatment information, and social security numbers.

6. Social security information and health related information of the type that was involved in this data breach is entitled to high level of protection due to its private and confidential

nature. The protection to which this information is entitled is recognized by statutory and case law, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The combination of this information with the names and birth dates of Plaintiff Foster and Data Breach Class members enhances the sensitivity of the information, making it susceptible to abuse and exploitation and requires the utmost protection in its handling.

7. Defendant HRS knew and understood the confidential and private nature of the Personal Information of Plaintiff Foster and Data Breach Class members and owed a duty to Plaintiff Foster and Data Breach Class members to protect and maintain the confidentiality of the Personal Information. In particular, social security numbers are a form of national identifier and are not easily replaced. Unlawful exploitation of social security numbers costs the federal government hundreds of millions of dollars a year from the fraudulent filing of tax returns by identity thieves and extols a severe financial toll on persons whose social security numbers are stolen and/or misappropriated.

8. The present case stems from the unauthorized access of Defendant HRS' computer storage systems. On February 5, 2019, Defendant HRS discovered that an unauthorized IP address had remotely accessed its computer network which contained the Personal Information of Plaintiff Foster and Data Breach Class members since November 14, 2019.

9. Despite Defendant HRS' duty to expeditiously notify individuals that their Personal Information may have been compromised, Defendant HRS kept its knowledge of the data breach secret from Plaintiff Foster and Data Breach Class members until releasing notification titled "NOTICE OF DATA INCIDENT" on April 5, 2019, roughly two months after Defendant discovered that the Personal Information of Plaintiff Foster and the Data Breach Class members had been compromised and misappropriated since November 14, 2018.

10. As a result of Defendant HRS' failure to adequately protect and secure the Personal Information in its possession and failure to timely detect the breach and failure to follow state and

federal laws related to protecting health information, unauthorized individuals gained and kept access to and obtained Personal Information belonging to Plaintiff Foster and Data Breach Class members. Once an unauthorized person or persons gain access to and steal this Personal Information, it can be used for improper purposes, including the theft of the identity of Plaintiff Foster and the Data Breach Class members, among other illicit purposes.

11. It is well known and the subject of many media reports that Personal Information data is highly coveted by and a frequent target of hackers and is often easily taken because it is inadequately protected. Legitimate organizations and the criminal underground alike recognize the value in Personal Information. Otherwise, they wouldn't pay for it or aggressively seek it. Personal Information data has been stolen and sold by the criminal underground on many occasions in the past. While Payment Card Industry data (PCI) is more regulated and protected than Personal Information, criminals are increasingly after Personal Information because they can use biographical data. Despite all of the publically available knowledge of the continued compromises of Personal Information, Defendant HRS' approach at maintaining the privacy of the Personal Information in its possession was lackadaisical, cavalier, reckless or at the very least negligent.

12. Defendant HRS' failure to maintain reasonable and adequate procedures to protect and secure the Personal Information and Defendant HRS' failure to timely discover the unauthorized access and failure to provide Plaintiff Foster and Data Breach Class members with timely information regarding the unauthorized access to their Personal Information, has resulted in financial injuries to Plaintiff Foster and Data Breach Class members, as well as Plaintiff Foster and Data Breach Class members being placed at grave risk of identity theft and other possible fraud and abuse.

13. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud." *See* 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at [www.javelinstrategy.com/brochure/276](http://www.javelinstrategy.com/brochure/276).

14. Identity thieves can use the type of Personal Information accessed in Defendant HRS' data breach to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit or credit cards.

15. Identity thieves can use Personal Information such as that pertaining to this Defendant HRS' data breach to perpetuate a variety of crimes that harm the victims. For instance, identity thieves may commit various types of government crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

16. In addition, identity thieves may get medical services using consumers' lost information or commit any number of other frauds, such as obtaining a job, procuring housing or even giving false information to police during an arrest.

17. Once Personal Information is stolen, the fraudulent use of that information and the resulting damage to consumers, and in this case, Plaintiff Foster and Data Breach Class members, may continue for years.

18. There is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning individuals whom Defendant HRS' had the Personal Information of could be at risk of fraud and identity theft for years into the future.

19. Plaintiff Foster and Data Breach Class members have suffered irreparable damage and will continue to suffer damages from the misuse of their Personal Information. As a proximate result of the unauthorized access, Plaintiff Foster and Data Breach Class members have had their Personal Information compromised, their privacy invaded, have incurred or will incur out-of-pocket costs and have otherwise suffered economic damages. Because of the data breach, Plaintiff Foster and the Data Breach Class have or should have their credit monitored by a professional credit monitoring service

such as LifeLock or Identity Guard. Because of the absence of adequate protection to safeguard the Personal Information of Plaintiff Foster and Data Breach Class members, protection through the issuance of an injunction against continued and future unauthorized intrusions and access is essential to safeguard the Personal Information of Plaintiff Foster and Data Breach Class members.

20. As a result of this breach, Plaintiff Foster has spent time taking steps to monitor his credit.

21. As a result of the breach, Plaintiff has had to incur costs related to monitor his credit.

22. Since the breach, Plaintiff has received multiple “credit alert” from Credit Karma, the latest on December 15, 2019.

23. As a result of the breach, Plaintiff has paid for a service, “PrivacyGuard,” to monitor his credit and will continue to incur costs related to credit monitoring.

24. HRS’s primary services include addiction testing and counseling and mental health counseling.

25. Because HRS’s primary services include mental health and substance abuse treatment, it is required to comply with the stringent requirements of 42 CFR Part 2.

26. HRS maintains medical records that include substance testing, mental health, and HIV status.

27. HRS conducts an initial patient intakes for new patients, including Plaintiff, which includes questions about substance abuse, mental health, and HIV status.

28. The breach involved the most sensitive health information related to their patients’ mental health history, substance abuse history, Sexually Transmitted Infection (STI) history, and Human Immunodeficiency Virus (HIV). history.

29. The mental health, substance abuse, STI, and HIV history combined with other personal information including social security numbers results in an unusually dangerous and damaging combination of disclosed personal and health information.

30. As a result of the disclosure of the most highly sensitive health information, Plaintiff and similarly situated patients of HRS have experienced irreparable harm and damages of a pecuniary and non-pecuniary nature, including the severe emotional distress resulting from having their most sensitive health information exposed.

31. Plaintiff expressly reserves the right to supplement this First Amended Complaint as other information relevant to this action becomes available.

### **CLASS DEFINITION AND RULE 23 ALLEGATIONS**

32. Plaintiff brings the Claims for Relief as class actions pursuant to Rule 23(a), (b)(2), and (b)(3). Plaintiff brings these claims on behalf of himself and all members of the following Class (“Data Breach Class”) comprised of:

#### **A. Data Breach Class**

All individuals residing in the United States whose Personal Information was compromised as a result of the data breach first disclosed by Defendant Health Recovery Services, Inc. on April 5, 2019.

33. The proposed class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

34. **Numerosity (Rule 23(a)(1)).** The proposed Data Breach Class includes many thousands of customers whose data was compromised in the data breach. While the precise number of Class members has not yet been determined, the massive size of the data breach indicates that joinder of each member would be impracticable.

35. **Existence of Common Questions of Law and Fact (Rule 23(a)(2)).** Common questions of law and fact exist and predominate over any questions affecting only individual Data Breach Class members. The common questions include:

- a. Whether or not Defendant HRS engaged in the conduct alleged herein;
- b. Whether or not Defendant HRS's conduct constituted deceptive trade practices actionable under the applicable consumer protection laws;
- c. Whether or not Defendant HRS had a legal duty to adequately protect Plaintiff Foster's and Data Breach Class members' Personal Information;
- d. Whether or not Defendant HRS breached its legal duty by failing to timely detect a data breach.
- e. Whether or not Defendant HRS breached its legal duty to adequately protect Plaintiff Foster's and Data Breach Class members' Personal Information;
- f. Whether or not Defendant HRS had a legal duty to provide timely and accurate notice of the data breach to Plaintiff Foster and Data Breach Class members;
- g. Whether or not Defendant HRS breached its duty to provide timely and accurate notice of the data breach to Plaintiff Foster and Data Breach Class members;
- h. If and when Defendant HRS knew or should have known that Plaintiff Foster's and Data Breach Class members' Personal Information stored on its computer systems was vulnerable to attack;
- i. Whether or not Plaintiff Foster and Data Breach Class members are entitled to recover actual damages and/or statutory damages; and
- j. Whether or not Plaintiff Foster and Data Breach Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

36. **Typicality (Rule 23(a)(3)).** Plaintiff Foster's claims are typical of the claims of the Data Breach Class. Plaintiff Foster and the Data Breach Class members were injured through

Defendant HRS' uniform misconduct and their legal claims arise from the same core Defendant HRS practices.

37. **Adequacy (Rule 23(a)(4)).** Plaintiff Foster is an adequate representative of the proposed Data Breach Class because his interests do not conflict with the interests of the Data Breach Class members he seeks to represent. Plaintiff Foster's counsel is very experienced in litigating consumer class actions and complex commercial disputes.

38. **Injunctive and Declaratory Relief (Rule 23(b)(2)).** Class certification of the Rule 23 claims is appropriate pursuant to Rule 23(b)(2) because Defendant HRS acted or refused to act on grounds generally applicable to the members of the Data Breach Class, making appropriate declaratory relief with respect to the members of the Data Breach Class as a whole.

39. **Predominance and Superiority of Class Action (Rule 23(b)(3)).** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Data Breach Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendant HRS. Even if it were economically feasible, requiring thousands of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

40. Finally, all members of the proposed Class are readily ascertainable. Defendant HRS has access to addresses and other contact information for thousands of members of the Class, which can be used to identify Data Breach Class members.

### **LEGAL CLAIMS**

#### **FIRST CLAIM FOR RELIEF Against Defendant Health Recovery Services, Inc.**

**BREACH OF CONFIDENCE: UNAUTHORIZED, UNPRIVILEGED DISCLOSURE  
TO A THIRD-PARTY OF NONPUBLIC MEDICAL INFORMATION  
(On Behalf of Plaintiff Foster and the Data Breach Class)**

41. Plaintiff Foster re-alleges all prior paragraphs of the Complaint as if set out here in full.

42. In Ohio, an independent tort exists for the unauthorized, unprivileged disclosure to a third party of non-public medical information that a physician or hospital has learned within a physician-patient relationship. *See Menorah Park Ctr. for Senior Living v. Rolston*, 2019 Ohio 2114 (Ohio App. 2019) citing *Biddle v. Warren Gen. Hosp.* (1999) 86 Ohio St. 3d 395.

43. Defendant made unauthorized and unprivileged disclosures to third parties of non-public medical information that a physician or hospital learned within a physician-patient relationship.

44. Plaintiff's and Data Breach Class members' private medical information stored on Defendant's system is nonpublic medical information. Defendant learned of that information through a physician-patient relationship.

45. Defendant had actual knowledge that it was vulnerable to a data breach prior to the breach. Defendant knowingly and intentionally failed to address the vulnerability prior to the breach that is the subject matter of this lawsuit. It only rebuilt its entire network after the data breach that is the subject matter of this lawsuit.

46. Plaintiff and members of the Data Breach Class did not and have not provided consent to Defendant to disclose their nonpublic medical information to any third party in the way described herein.

47. As a result of the breach, the Plaintiff's and the putative class members' protected health information was disclosed to an unauthorized third party, who had access to the information from on or about November 14, 2018 through February 5, 2018.

48. Defendant failed to use reasonable efforts to limit disclosure of the protected health information.

49. As a result of the foregoing, Plaintiff Foster and the Data Breach Class have suffered injury and are entitled to damages in an amount to be proven at trial.

**SECOND CLAIM FOR RELIEF**  
**Against Defendant Health Recovery Services, Inc.**  
**Violation of Ohio Consumer Sales Practices Act (Ohio Rev. Code § 1345.01 *et seq.*)**  
**(On Behalf of Plaintiff Foster and the Data Breach Class)**

50. Plaintiff Foster re-alleges all prior paragraphs of the Complaint as if set out here in full.

51. Plaintiff Foster brings this claim on behalf of himself and the Data Breach Class.

52. The Ohio Consumer Sales Practices Act (Ohio CSPA), Ohio Rev. Code § 1345.02 *et seq.*, broadly prohibits unfair or deceptive acts or practices in connection with a consumer transaction. Specifically, and without limitation of the broad prohibition, the Act prohibits (1) representing that the products and services of Defendant HRS have characteristics, uses, benefits, and qualities which they do not have, (2) representing that the products and services of Defendant HRS are of a particular standard, quality, and grade when they are not, (3) advertising the products and services of Defendant HRS with the intent not to sell them as advertised, and (4) engaging in acts or practices which are otherwise unfair, misleading, false, or deceptive to the consumer.

53. Defendant is a “supplier” as that term is defined in Ohio Rev. Code § 1345.01(C).

54. Plaintiff Foster and the Data Breach Class members are “consumers” as that term is defined in Ohio Rev. Code § 1345.01(D), and their use of the products and services of Defendant HRS are “consumer transactions” within the meaning of Ohio Rev. Code § 1345.01(A).

55. Defendant misrepresented Plaintiff and the Data Breach Class and/or and/or mislead Plaintiff and the Data Breach Class and/or unfairly misrepresented to Plaintiff and the Data Breach

Class that it maintained its computer network in compliance with state and federal law and in compliance with industry custom.

56. As a result of the foregoing wrongful conduct, Plaintiff Foster and the Data Breach Class have been damaged in an amount to be proven at trial and seek all just and proper remedies, including but not limited to actual and statutory damages, court costs, and reasonable attorneys' fees, pursuant to Ohio Rev. Cod § 1345.09 *et seq.*

**THIRD CLAIM FOR RELIEF**  
**Against Defendant Health Recovery Services, Inc.**  
**Negligence**  
**(On Behalf of Plaintiff Foster and the Data Breach Class)**

57. Plaintiff Foster re-alleges all prior paragraphs of the Complaint as if set out here in full.

58. Plaintiff Foster brings this claim on behalf of himself and the Data Breach Class.

59. Defendant HRS solicited, gathered, and stored Personal Information (including, but not limited to names, addresses, telephone numbers, dates of birth, medical information, health insurance information, diagnoses, treatment information, and social security numbers) of its patients, including Plaintiff Foster and the Data Breach Class.

60. Defendant HRS knew, or should have known, the risks inherent in collecting and storing the Personal Information of Plaintiff Foster and the Data Breach Class and the importance of adequate security. Defendant HRS knew, or should have known, about other publicized data breaches at other health care providers, agencies, and businesses.

61. Pursuant to O.R.C. 3798.03(A)(2), Defendant owed Plaintiff a duty to implement and maintain appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information in a manner consistent with federal and state regulations, including but not limited to 45 C.F.R. 164.306(c) and 45 C.F.R. 164.530(c).

62. Defendant HRS owed duties of care to Plaintiff Foster and the Data Breach Class whose Personal Information was entrusted to it. Defendant HRS's duties included the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting the Personal Information of its patients;
- b. To protect patients' Personal Information using reasonable and adequate security procedures and systems that are compliant with Ohio laws and consistent with industry-standard practices;
- c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- d. To promptly notify patients of the data breach.

63. Because Defendant HRS knew that a breach of its systems would damage its more than 20,000 patients, including Plaintiff Foster and the Data Breach Class, it had a duty to adequately protect their Personal Information.

64. Defendant HRS owed a duty of care to not subject Plaintiff Foster and the Data Breach Class to an unreasonable risk of harm because they were foreseeable and probably victims of any inadequate security practices.

65. Defendant HRS knew, or should have known, that its computer systems did not adequately safeguard the Personal Information of Plaintiff Foster and the Data Breach Class.

66. Defendant HRS breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Personal Information of Plaintiff Foster and the Data Breach Class.

67. Defendant failed to maintain their computer property in a manner that honored their duties and promises to Plaintiff and Data Breach Class members. In particular, Defendant was negligent in one or more of the following ways:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect patients' Personal Health Information and other Personal Information;
- c. Failing to properly monitor their own data security systems for existing intrusions;
- d. Failing to ensure that their vendors with access to their computer and data systems properly employed reasonable data security procedures;
- e. Failing to ensure the confidentiality and integrity of electronic of electronic protected health information (PHI) they created, maintained, and/or transmitted in violation of 45 C.F.R. 164.306(a)(1);
- f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. 164.312(a)(1).
- g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. 164.308(a)(1)(i);
- h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. 164.308(a)(1)(ii)(D);
- i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);
- j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. 164.306(a)(3);

- k. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. 164.306(a)(4); and/or
- l. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. 164.530(b).

68. Defendant HRS acted with reckless disregard for the security of the Personal Information of Plaintiff Foster and the Data Breach Class because Defendant HRS knew or should have known that its computer systems and data security practices were not adequate to safeguard the Personal Information that it collected and stored, which unauthorized persons were attempted to, or did access.

69. Defendant HRS acted with reckless disregard for the rights of Plaintiff Foster and the Data Breach Class by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use of the Personal Information compromised in the data breach by unauthorized persons.

70. Defendant HRS had a special relationship with Plaintiff Foster and the Data Breach Class. Plaintiff Foster's and the Data Breach Class' willingness to entrust Defendant HRS with their Personal Information was predicated on the understanding that Defendant HRS would take adequate security precautions to protect that Personal Information. Moreover, only Defendant HRS had the ability to protect its systems (and the Personal Information that it stored on them) from attack.

71. If not for Defendant HRS' wrongful and negligent breach of the duties it owed Plaintiff Foster and the Data Breach Class, their personal information either would not have been compromised and they would have been able to prevent some or all of their damages.

72. As a direct and proximate result of Defendant HRS' negligent conduct, Plaintiff Foster and the Data Breach Class have suffered damages and are at imminent risk of further harm.

73. The injury and harm that Plaintiff Foster and the Data Breach Class members suffered (as alleged above) was reasonably foreseeable.

74. The injury and harm that Plaintiff Foster and the Data Breach Class members suffered (as alleged above) was the direct and proximate result of Defendant HRS' negligent conduct.

75. As a result, Plaintiff Foster and the Data Breach Class have suffered injury and are entitled to damages in an amount to be proven at trial.

**FOURTH CLAIM FOR RELIEF**  
**Against Defendant Health Recovery Services, Inc.**  
**Breach of Contract**  
**(On Behalf of Plaintiff Foster and the Data Breach Class)**

76. Plaintiff Foster re-alleges all prior paragraphs of the Complaint as if set out here in full.

77. Plaintiff Foster brings this claim on behalf of himself and the Data Breach Class.

78. Plaintiff Foster and the Data Breach Class members are parties to express agreements with Defendant HRS whereby Plaintiff Foster and the Data Breach Class members provide their Personal Information to Defendant HRS in order to receive Defendant HRS' services, including the provision of reasonable safeguards to prevent the unauthorized disclosure of Plaintiff Foster's and the Data Breach Class members' Personal Information.

79. Defendant HRS' failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures constitutes a breach of a contract between Defendant and Plaintiff Foster and the Data Breach Class members.

80. Plaintiff Foster and the Data Breach Class members relied upon Defendant HRS' representations that it would keep their Personal Information private and secure.

81. Plaintiff Foster and the Data Breach Class members performed their obligations by providing their Personal Information to Defendant HRS in connection with receiving Defendant HRS' services.

82. Defendant HRS breached its obligation to maintain adequate safeguards to protect the privacy and security of Plaintiff Foster and the Data Breach Class members.

83. As a direct and proximate result of Defendant HRS' breach of its contractual obligations, Plaintiff Foster and the Data Breach Class have suffered damages and are at imminent risk of further harm.

**FIFTH CLAIM FOR RELIEF**  
**Against Defendant Health Recovery Services, Inc.**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiff Foster and the Data Breach Class)**

84. Plaintiff Foster re-alleges all prior paragraphs of the Complaint as if set out here in full.

85. Plaintiff Foster brings this claim on behalf of himself and the Data Breach Class.

86. Plaintiff Foster and the Data Breach Class members were required to provide Defendant HRS their Personal Information in order to receive Defendant HRS' services. To the extent that it is found that Defendant HRS did not have an express contract with Plaintiff Foster and the Data Breach Class members, Defendant HRS entered into implied contracts with Plaintiff Foster and the Data Breach Class members whereby, by virtue of such requirement to provide their Personal Information, Plaintiff and the Data Breach Class members entered into implied contracts whereby Defendant HRS was obliged to take reasonable steps to secure and safeguard such Personal Information.

87. Defendant HRS' failure to implement an adequate and reasonable data privacy and cybersecurity protocol which included adequate prevention, detection, and notification procedures

constitutes a breach of an implied contract between Defendant and Plaintiff Foster and the Data Breach Class members.

88. Plaintiff Foster and the Data Breach Class members performed their obligations by providing their Personal Information to Defendant HRS in connection with receiving Defendant HRS' services.

89. Defendant HRS breached its obligation to maintain adequate safeguards to protect the privacy and security of Plaintiff Foster and the Data Breach Class members.

90. As a direct and proximate result of Defendant HRS' breach of its contractual obligations, Plaintiff Foster and the Data Breach Class have suffered damages and are at imminent risk of further harm.

**SIXTH CLAIM FOR RELIEF**  
**Against Defendant Health Recovery Services, Inc.**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff Foster and the Data Breach Class)**

91. Plaintiff Foster re-alleges all prior paragraphs of the Complaint as if set out here in full.

92. Plaintiff Foster brings this claim on behalf of himself and the Data Breach Class.

93. Plaintiff Foster and the Data Breach Class members conferred a benefit to Defendant HRS when they entered into a contractual agreement with Defendant HRS and provided payment for Defendant HRS' services.

94. In exchange for, and in consideration of, Plaintiff Foster and the Data Breach Class members providing payment for Defendant HRS' services, Defendant HRS was required to, and Plaintiff Foster and the Data Breach Class members expected Defendant HRS to, implement reasonable security policies and procedures that would have protected Plaintiff Foster's and the Data Breach Class members' Personal Information.

95. To the extent that Defendant HRS devotes financial resources to the protection of its patients Personal Information, a portion of those financial resources are derived from the benefit conferred by contractual payments made by Plaintiff Foster and the Data Breach Class members to Defendant HRS.

96. As a result of Defendant HRS' acts and omissions as alleged herein, Defendant HRS has been unjustly enriched to the extent that any portion of such contractual payments comprises spending for adequate security not provided.

**SEVENTH CLAIM FOR RELIEF**  
**Against Defendant Health Recovery Services, Inc.**  
**2307.60 Civil Action for Damages for Criminal Act**  
**(On Behalf of Plaintiff Foster and the Data Breach Class)**

97. Plaintiff Foster re-alleges all prior paragraphs of the Complaint as if set out here in full.

98. Plaintiff Foster brings this claim on behalf of himself and the Data Breach Class.

99. As a result of both HRS's failure to protect to comply with HIPAA as well as the unauthorized access of Plaintiff's PHI, Plaintiff and the Data Breach Class are victims of a criminal act as defined by ORC 2307.60.

100. A non-exhaustive list of criminal acts in which Plaintiff and the Data Breach Class are victims are as follows:

- a. ORC 2913.04
- b. ORC 2913.02
- c. 18 USC §1030
- d. 42 USC §1320d-5
- e. 42 USC §1320d-6

101. As a result of the foregoing wrongful conduct, Plaintiff Foster and the Data Breach Class have been damaged in an amount to be proven at trial and seek all just and proper remedies,

including but not limited to actual and statutory damages, court costs, and reasonable attorneys' fees, pursuant to Ohio Rev. Cod § 2307.60 *et seq.*

**EIGHTH CLAIM FOR RELIEF  
Against Defendant Health Recovery Services, Inc.  
Willful Violation of the Fair Credit Reporting Act  
(On Behalf of Plaintiff Foster and the Data Breach Class)**

102. Plaintiff repeats and re-allege all paragraphs as if fully set forth herein.

103. Plaintiff Foster brings this claim on behalf of himself and the Data Breach Class.

104. One of the fundamental purposes of FCRA is to protect consumers' privacy.

105. U.S.C. § 1681(a). Protecting consumers' privacy involves adopting reasonable procedures to keep sensitive information confidential.

106. FCRA defines a "consumer reporting agency" as:

[A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. 15 U.S.C. § 1681a(f).

107. FCRA defines a "consumer report" as:

[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under [15 U.S.C. §] 1681(b). 15 U.S.C. § 1681a(d)(1).

108. On a cooperative nonprofit basis or for monetary fees, Defendant regularly assembles consumer information including, among other things, insurance policy information, such as names, dates of birth, and Social Security Numbers of those insured; claims information, such as the date of loss, type of loss, and amount paid for claims submitted by an insured; and a description of insured items. Defendant also regularly utilizes interstate commerce to furnish such information on consumers (consumer reports) to third parties.

109. Plaintiff and Class Members' Personally Identifiable Information (PII) and Protected Health Information (PHI) constitute Consumer Reports under FCRA, because this information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiff's and the other Class Members' eligibility for insurance to be used primarily for personal, family, or household purposes, and establishing rates for same.

110. FCRA requires the adoption of reasonable procedures with regard to, *inter alia*, the confidentiality and proper utilization of personal and insurance information. 15 U.S.C. § 1681(b). FCRA also requires that consumer reporting agencies "maintain reasonable procedures designed to ... limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e.

111. Defendant failed to adopt and maintain these and other reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b.

112. Defendant failed to take reasonable and appropriate measures to secure the network and safeguard and protect Plaintiff and Class Members' PII/PHI. Defendant also failed to place itself in a position to immediately notify Plaintiff and Class Members about the Data Breach.

113. FCRA defines "medical information" as:

[I]nformation or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—(A) the past, present, or future physical, mental, or behavioral health or condition of an individual; (B) the provision of health care to an individual; or (C) the payment for the provision of health care to an individual. 15 U.S.C. § 1681a(i).

114. FCRA specifically protects medical information, restricting its dissemination to limited instances. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

115. Plaintiff and Class Members' PHI affected by the Data Breach constitutes medical information as defined by FCRA. Their PHI included enrollment and clinical information, which constitute data relating to the provision of health care and past, present, or future physical, mental, or behavioral health or condition of an individual under FCRA's definition of medical information. *See* 15 U.S.C. § 1681a(i).

116. Under FCRA, a "person that receives medical information [in connection with the business of insurance or annuities] shall not disclose such information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order." 15 U.S.C. §§ 1681b(g)(4), 1681b(g)(3)(A).

117. Because Defendant is a person that receives medical information in connection with their business, under FCRA, Defendant shall not disclose such information to any other person except as necessary to carry out the purpose for which it received the information or as permitted by statute, regulation, or order. *See* 15 U.S.C. §§ 1681b(g)(4), 1681b(g)(3)(A).

118. Defendant's failure to protect and safeguard the PII/PHI of Plaintiff and Class Members resulted in the disclosure of such information to one or more third-parties in violation of FCRA because such disclosure was not necessary to carry out the purpose for which Defendant received the information, nor was it permitted by statute, regulation, or order.

119. Defendant's violations of FCRA, as set forth above, were willful or, at the very least, reckless, constituting willfulness. Defendant willfully failed to encrypt or otherwise adequately protect Plaintiff's and Class Members' PII/PHI.

120. As a result of Defendant's willful or reckless failure to adopt and maintain reasonable procedures to limit the furnishing of Plaintiff's and Class Members' PII to the purposes listed under 15 U.S.C. § 1681b, Plaintiff's and the other Class Members' PII was disseminated to unauthorized third parties, compromised, and stolen. Plaintiff's suffered individual harm as a result of Defendant's willful or reckless

violations of FCRA.

121. As a further direct or proximate result of Defendant's willful or reckless violations of FCRA, as described above, Plaintiff and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) damages.

122. Plaintiff and Class Members, therefore, are entitled to compensation for their actual damages or statutory damages of not less than \$100, and not more than \$1,000, each, as well as attorneys' fees, punitive damages, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

**NINTH CLAIM FOR RELIEF**  
**Against Defendant Health Recovery Services, Inc.**  
**Negligent Violation of the Fair Credit Reporting Act**  
**(On Behalf of Plaintiff Foster and the Data Breach Class)**

123. Plaintiff repeats and re-alleges all preceding paragraphs as if fully set forth herein.

124. Plaintiff Foster brings this claim on behalf of himself and the Data Breach Class.

125. Defendant negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b.

126. Plaintiff and the other Class Members' PII/PHI was wrongfully disseminated to the public as a direct and foreseeable result of Defendant's failure to adopt and maintain such reasonable procedures.

127. Defendant disclosed medical information to one or more third-parties in violation of FCRA because such disclosure was not necessary to carry out the purpose for which Defendant received the information, nor was it permitted by statute, regulation, or order.

128. As a direct or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiff and Class Members' PII/PHI was made accessible to unauthorized third parties in the public domain, compromised, and stolen. Plaintiff suffered individual harm as a result of Defendant's negligent violations of FCRA.

129. As a further direct or proximate result of Defendant's negligent violations of FCRA,

as described above, Plaintiff and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages.

130. Plaintiff and the other Class Members, therefore, are entitled to compensation for their actual damages as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C. § 1681o.

**TENTH CLAIM FOR RELIEF**  
**Against Defendant Health Recovery Services, Inc.**  
**Violation of Ohio Rev. Code Ann. § 3701.243**  
**(On Behalf of Plaintiff Foster and the Data Breach Class)**

131. The Plaintiff repeats and re-allege all of the allegations of the preceding Paragraphs as if fully incorporated and set forth herein.

132. At all times material herein Defendant has been subject to the requirements of § 3701.243.

133. Ohio law prohibits disclosing any record related to HIV status to be disclosed without written consent or without statutorily enumerated authorization. Ohio Rev. Code Ann. § 3701.243.

134. As a result of the breach, Defendant disclosed the HIV status of Class Members without these Class members' advance written authorization.

135. These disclosures were made in connection with the provision of health care services in this State. Defendant violated Ohio law by disclosing, without receiving advance authorization from the Plaintiff or any Class members:

(1) The identity of any individual on whom an HIV test is performed; (2) The results of an HIV test in a form that identifies the individual tested; [or] (3) The identity of any individual diagnosed as having AIDS or an AIDS-related condition.

and without the required disclosures, in violation of Ohio Rev.Code § 3701.243(A)(1)-(3) and (E).

136. As a direct and proximate result of Defendant's actions, the Plaintiff and Class

members have suffered damages.

137. The Plaintiff and Class members have a private right of action for Defendant's violations of this law. Ohio Rev. Code § 3701.244(B).

138. The Plaintiff and Class members seek relief, including but not limited to damages, punitive damages, injunctive relief, declaratory judgment, and attorneys' fees and costs.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff Foster, on behalf of himself and the Data Breach Class described above, respectfully asks the Court for the following relief:

- (a) An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff Foster is proper representative of the Class requested herein;
- (b) A judgment in favor of Plaintiff Foster and the Data Breach Class awarding them appropriate monetary relief, including actual damages, compensatory damages, punitive damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;
- (c) An order requiring Defendant HRS to pay for Plaintiff Foster and the Data Breach Class members to receive credit monitoring and identity theft protection;
- (d) An order providing injunctive and other equitable relief as necessary to protect the interests of the Data Breach Class as requested herein;
- (e) An order requiring Defendant HRS to pay the costs involved in notifying the Data Breach Class members about the judgment and administering the claims process;

- (f) A judgment in favor of Plaintiff Foster and the Data Breach Class awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law;
- (g) Statutory and liquidated damages; and
- (h) An award of such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

139. Plaintiff demands a trial by jury on all triable issues.

DATED: January 6, 2020

Respectfully submitted,

s/ Michael L. Fradin  
Attorney for Plaintiff Foster

LAW OFFICE OF MICHAEL L. FRADIN  
Michael L. Fradin, Esq.  
8401 Crawford Ave. Ste. 104  
Skokie, IL 60076  
Telephone: 847-986-5889  
Facsimile: 847-673-1228  
Email: mike@fradinlaw.com

**CERTIFICATE OF SERVICE**

This will certify that the foregoing was filed electronically on January 6, 2020. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

*s/ Michael Fradin*

---

Michael L. Fradin (0091739)